PhishMe Reporter™

REAL THREATS IN REAL-TIME FROM EMPLOYEES

PHISHME

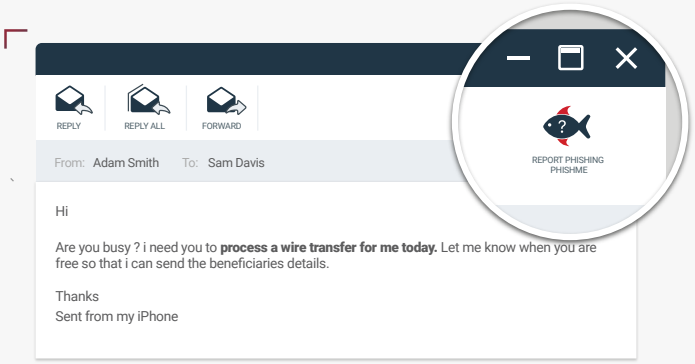
Though PhishMe Simulator conditions employees to resist phishing attempts, “not clicking” isn’t enough. During a phishing attack, early detection matters. Visibility is critical for security operations and incident response teams to minimise the time an attacker is on your network. PhishMe Reporter™ provides organisations with a simple, cost-effective way to generate user reports of suspicious emails that may indicate early stages of a cyber attack.

Why choose PhishMe Reporter™?

PhishMe has been proven to reduce the threat of employees falling victim to advanced cyber attacks by up to 95% – preparing your last line of defence to recognise and resist tricky phishing attempts.

Key Benefits

- ✓ Standardise and organise your user reporting process
- ✓ Detect and respond to email-based threats faster with user-generated reporting
- ✓ Analyse URL and malware attachments using third-party integrations
- ✓ Minimise impact of breaches with proactive response and improved visibility
- ✓ Customisable user feedback encourages employees to be a part of the security process



What is PhishMe Reporter™?

When technical defences such as proxy filtering, URL rewriting, and DLP fail, users are the last line of defence. Armed with the proper training, users can provide timely and valuable threat intelligence simply by recognising and reporting suspicious emails. Organisations have struggled to tap into this resource and, consequently, malicious activities often operate for weeks and even months on the network.

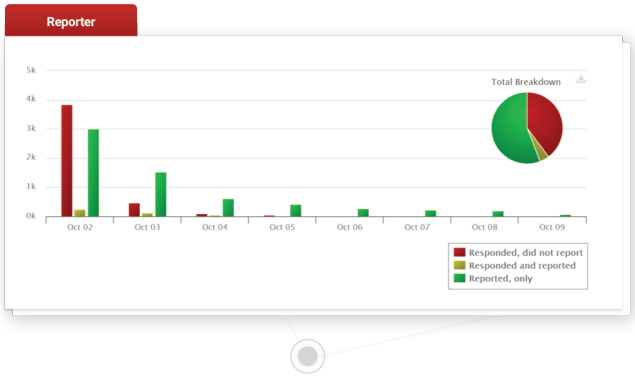
PhishMe Reporter streamlines the reporting process by installing an email add-in on users’ email toolbars that, when clicked, sends a suspicious email to your security team containing the relevant information needed to analyse and respond.

Reporter automatically discerns emails reported from PhishMe Simulator scenarios and emails reported from unknown sources, ensuring that only reports of potentially malicious emails are delivered to appropriate security staff or PhishMe Triage for analysis.

Enhanced Reporting

Whether or not you have a reporting process in place, Reporter can help you improve by:

- Preserving the full header of reported emails, allowing responders to block and remove similar emails.
- Ensuring any attachments and URLs are included.
- Supplementing Simulator campaigns, tracking user responses and organisational time to response.



Is this email a PhishMe scenario?

YES, IT IS. ?

▼

RECORD USER REPORT IN PHISHME

▼

PRESENT "THANK YOU" DIALOGUE USER

CLICK !

"What happens when I push the button...?"

NO, IT'S THE REAL DEAL. ?

▼

REPORT EMAIL TO IR

▼

PRESENT "THANK YOU" DIALOGUE USER

▼

SEND TO TRIAGE OR INTERNAL SECURITY TEAM FOR ANALYSIS AND DETERMINATION ON COURSE OF ACTION

PhishMe Simulator Emails

Reporter collects reports of emails sent from Simulator, noting which users reported them and providing the user with customisable acknowledgement of the successful report. Positive reinforcement in the feedback loop further enhances employees' capabilities to accurately identify cyber attacks. This information is tracked and integrated into the PhishMe solution's comprehensive reporting metrics.

Suspicious Unknown Emails

Reports of suspicious unknown emails are forwarded to a designated location or Triage, where they can be analysed by an organisation's internal security team. Suspicious emails are attached with the original header and contextual information for rapid analysis. Incident response and security operations teams can prioritise their analysis based on a user's reputation for accurately identifying phishing attempts among other attributes when using Triage.

PhishMe is the leading provider of human-focused phishing defence solutions for organisations concerned about their susceptibility to today's top attack vector — spear phishing. PhishMe's intelligence-driven platform turns employees into an active line of defence by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats. Our open approach ensures that PhishMe integrates easily into the security technology stack, demonstrating measurable results to help inform an organisation's security decision making process. PhishMe's customers include the defence industrial base, energy, financial services, healthcare, and manufacturing industries, as well as other Global 1000 entities that understand changing user security behaviour will improve security, aid incident response, and reduce the risk of compromise.

PHISHME

For more information contact:

W: phishme.com/contact T: 703.652.0717

A: 1608 Village Market Blvd, SE #200 Leesburg, VA 20175